Applicant: Mike C. Robinson et al.
Serial No.: 10/061,619
Filed: February 1, 2002
Docket No.: 100200201-1
Title: SECURE INITIALIZATION OF COMMUNICATION WITH A NETWORK RESOURCE

REMARKS

The following Remarks are made in response to the Final Office Action mailed July 3, 2007, in which claims 1-6, 13-30, and 36-51 were rejected.

With this Amendment, claims 1, 5, 13, 17, 19, 26, 30, 36, 40, 41, 45, 47, and 51 have been amended to clarify Applicant's invention.

Claims 1-6, 13-30, and 36-51 remain pending in the application and are presented for reconsideration and allowance.

Claim Rejections under 35 U.S.C. § 112

Clams 1-6, 13-30, and 36-51 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement in that the Examiner contends that the claim(s) contain subject matter, which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. More specifically, the Examiner contends that the specification discloses receiving an access, but does not explicitly disclose receiving "unsecured" access to the network and responding to the "unsecured" access as amended.

With this Amendment, independent claim 1 has been amended to clarify that the method includes **"receiving access in an unsecured mode to the network resource from a management application of the client via the network;"** and **"in the unsecured mode, generating configuration parameters for initializing secure communication between the network resource and the client via the network."**

With this Amendment, independent claim 13 has been amended to clarify that the system includes **"means for receiving access in an unsecured mode to the network resource from a management application of the client via the network;"** and **"means for generating configuration parameters for initializing secure communication between the network resource and the client via the network, while in the unsecured mode."**

With this Amendment, independent claim 19 has been amended to clarify that the system includes **"a network interface configured to receive access in an unsecured mode via the network from a management application of the client;"** and **"an SNMP daemon configured to generate configuration parameters for initializing secure communication with the client via the network, while in the unsecured mode."**

With this Amendment, independent claim 26 has been amended to clarify that the method includes **"receiving ad hoc access in an unsecured mode to the network resource from a management application of the client;"** and **"in the unsecured mode, generating a security key for initializing secure communication between the network resource and the client via a wireless access point."**

With this Amendment, independent claim 36 has been amended to clarify that the system includes **"means for receiving ad hoc access in an unsecured mode to the network resource from a management application of the client;"** and **"means for generating a security key for initializing secure communication between the network resource and the client via a wireless access point while in the unsecured mode."**

With this Amendment, independent claim 41 has been amended to clarify that the method includes **"receiving access in an unsecured mode to the network resource from a management application of the client via the network;"** and **"in the unsecured mode, generating configuration parameters for initializing secure communication between the network resource and the client via the network."**

With this Amendment, independent claim 47 has been amended to clarify that the method includes **"receiving ad hoc access in an unsecured mode to the network resource from a management application of the client;"** and **"in the unsecured mode, generating a security key for initializing secure communication between the network resource and the client via a wireless access point."**

Applicant notes that support for these amendments is provided, for example, at page 12, lines 8-15 of the Specification which provide that:

> *It should be noted that the configuration information provided by the security configuration page 130 is provided to the user without exposure across a network 103* ***in an unsecured mode****. This allows the user to access network resource 102 in a more convenient* ***unsecured mode*** *(e.g., SNMPv1) in order to obtain the security configuration page 130, and then subsequently initiate secure communication after configuring the management application 110* (emphasis added).

And, at page 12, lines 15-29 of the Specification which provide that:

> *In this manner, embodiments of the present invention provide a solution that protects sensitive network resources, such as print servers*

> *and the like, while retaining the ability to accommodate new users. New users are still able to access* ***unsecured*** *areas or insensitive areas of network 103 while remaining* ***in an unsecured mode****. Once the user requires access to a high value network resource (e.g., network resource 102) the user to requests a security configuration page 130 and configure his/her client 101 accordingly (e.g., via the management application 110). Once secure communication is initialized, the embodiments of the present invention protect against common network attacks such as spoofing, packet sniffing, and the like. In this manner, embodiments of the present invention provide access to those individuals requiring it, while simultaneously preventing and denying access to those who are not authorized* (emphasis added).

Accordingly, Applicant submits that receiving access in an "unsecured mode" to the network and generating configuration parameters or a security key for initializing secure communication while in the "unsecured mode" was described in the Specification.

Applicant, therefore, respectfully requests that the rejection of claims 1-6, 13-30, and 36-51 under 35 U.S.C. 112, first paragraph, be reconsidered and withdrawn, and that claims 1-6, 13-30, and 36-51 be allowed.

RECEIVED
CENTRAL FAX CENTER
OCT 03 2007

CONCLUSION

In view of the above, Applicant respectfully submits that pending claims 1-6, 13-30, and 36-51 are all in a condition for allowance and requests reconsideration of the application and allowance of all pending claims.

Any inquiry regarding this Amendment and Response should be directed to either Nathan R. Rieth at Telephone No. (208) 396-5287, Facsimile No. (208) 396-3958 or Scott A. Lund at Telephone No. (612) 573-2006, Facsimile No. (612) 573-2005. In addition, all correspondence should continue to be directed to the following address:

IP Administration
Legal Department, M/S 35
HEWLETT-PACKARD COMPANY
P.O. Box 272400
Fort Collins, Colorado 80527-2400

Respectfully submitted,

Mike C. Robinson et al.,

By,

DICKE, BILLIG & CZAJA, PLLC
Fifth Street Towers, Suite 2250
100 South Fifth Street
Minneapolis, MN 55402
Telephone: (612) 573-2006
Facsimile: (612) 573-2005

Date: Oct. 3, 2007
SAL:hsf

Scott A. Lund
Reg. No. 41,166

CERTIFICATE UNDER 37 C.F.R. 1.8: The undersigned hereby certifies that this paper or papers, as described herein, are being facsimile transmitted to the United States Patent and Trademark Office, Fax No. (571) 273-8300 on this 3rd day of October, 2007.

By
Name: Scott A. Lund